

UNITED STATES DISTRICT COURT

for the

Eastern District of California

FILED

Feb 18, 2025

CLERK, U.S. DISTRICT COURT
EASTERN DISTRICT OF CALIFORNIA

SEALED

In the Matter of the Search of)

2484 AMELIA EARHART AVENUE,
SACRAMENTO, CALIFORNIA 95834)

Case No.

2:25-sw-0135 JDP

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (*identify the person or describe the property to be searched and give its location*):

SEE ATTACHMENT A-2, attached hereto and incorporated by reference,

located in the Eastern District of California, there is now concealed:

SEE ATTACHMENT B, attached hereto and incorporated by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 1343	Wire fraud
18 U.S.C. § 1344	Bank fraud
18 U.S.C. § 1957	Conducting monetary transactions with proceeds of unlawful activity

The application is based on these facts:

SEE AFFIDAVIT, attached hereto and incorporated by reference.

- ☐ Continued on the attached sheet.
- ☐ Delayed notice _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ Marshall Miller

Applicant's signature

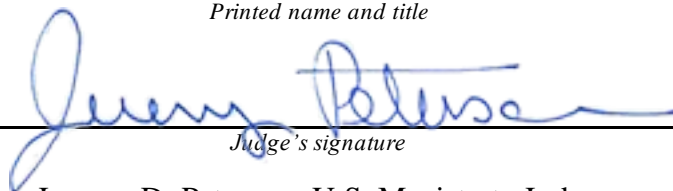
Marshall Miller, IRS-CI Special Agent

Printed name and title

Sworn to and signed telephonically.

Date: February 18, 2025

City and state: Sacramento, California



Judge's signature

Jeremy D. Peterson, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

I, Marshall Miller, being first duly sworn, hereby depose and state as follows:

I. INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for warrants to search the person of Akash Kumar Singh (“Singh”) and the premises at 2484 Amelia Earhart Avenue, Sacramento, California 95834 (the “Subject Premises”), further described in Attachments A-1 and A-2, which are incorporated by reference. Based on my training and experience and the facts as set forth in this affidavit, I submit that there is probable cause to believe that Singh has violated 18 U.S.C. §§ 1343, 1344, and 1957, and that evidence, instrumentalities, contraband, and fruits of these criminal violations will be found on his person and inside the Subject Premises. Hence, the warrants for which I am applying seek authorization to search Singh and the Subject Premises—including any computers, cellular devices, or other electronic storage media inside the Subject Premises that reasonably appear to belong to Singh or to contain evidence called for by the warrants for which I am applying—for the things described in Attachment B.

2. I am a Special Agent with Internal Revenue Service-Criminal Investigation, and have been since 2018. My duties include the investigation of criminal violations of the Internal Revenue Code, anti-money laundering statutes, and other related offenses. My professional training consisted of approximately twenty-six weeks of training at the Federal Law Enforcement Training Center in Glynco, Georgia, which included training in law enforcement techniques, federal criminal statutes, conducting criminal investigations, and the execution of search, seizure, and arrest warrants. I have also received training in financial investigative techniques, legal principles, and statutes representing criminal violations of the United States Code as enumerated in Titles 18, 26, and 31. Furthermore, I have a master’s degree in accounting from the University of California at Davis and a bachelor’s degree in criminology from the University of California at Irvine.

3. I have led or been involved in numerous investigations of money laundering, health-care fraud, wire fraud, bank fraud, conspiracy, tax evasion, and other related offenses. I

have led or participated in numerous interviews and have been the affiant for multiple federal search warrants involving suspected criminal violations authorizing seizure of records of the type involved in this investigation. I have personally authored affidavits in support of warrants for the seizure of property that constituted the proceeds of money laundering or fraud under the forfeiture statutes found within Title 18 of the United States Code. I have personally traced the proceeds of fraud between financial accounts, utilizing various accounting methods to determine the balance of fraud proceeds held within certain accounts on a given date.

4. I am currently assigned to the Eastern District of California COVID-19 Fraud Strike Force, a cooperative effort involving the Federal Bureau of Investigation, the Department of Labor, the Small Business Administration, and other allied law enforcement agencies. Furthermore, I have led multiple investigations of COVID-19 fraud-related schemes since 2020. I have served as the affiant on multiple COVID-19 fraud-related search warrants and conducted seizures of property for forfeiture derived from COVID-19 fraud. Thus, I am familiar with COVID-19 fraud schemes and how they are carried out.

5. Based on my training and experience and that of others with whom I work, I am familiar with the methods and practices used by individuals and organizations engaged in financial crimes. These individuals often maintain records of their financial activities, such as bank records, receipts, and documentation of expenditures, notes, or correspondence, negotiated instruments, contracts, and other financial documents, within their personal residence and within electronic devices or papers carried upon their person. I am aware that individuals engaged in financial crimes commonly participate in these activities for profit. It is common for the proceeds of financial crimes to be in the form of cash, negotiable instruments, or other assets, which are also frequently kept inside residences or in electronic form on computers and electronic devices.

6. Furthermore, based on my training and experience, I know that it is common for persons engaging in financial crimes to invest the profits in other assets, reduce current or long-term liabilities, convert the profits to other forms of financial instruments, and/or pay personal expenditures. I am aware that such transactions, transfers, or expenditures of criminally derived

profits cause the creation of numerous types of documents, which reflect the fruits of financial crimes. Documents such as bank records, cashier's check records, receipts, invoices, expenditure records, escrow documents, notes or notations, and other similar documents are frequently generated upon the transactions, transfers, and/or expenditures of criminally derived funds, and are frequently stored in paper format inside residences or in electronic format inside computers and other electronic devices. I know from training and experience, and the experience of other law enforcement officers with whom I work, that correspondence or records related to these financial activities are commonly kept in the personal residence or within electronic devices or papers carried upon the person of individuals engaging in criminal activities related to wire fraud, bank fraud, and money laundering.

7. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrants and does not reflect all information I have received or know about this matter. Further, I do not have personal knowledge of all the matters set forth in this affidavit. To the extent that any information in this affidavit is not within my personal knowledge, it was made known to me through my own review of documents discussed in this affidavit, through interviews of knowledgeable persons, and through reliable law enforcement sources, including discussions with other law enforcement agents.

8. Moreover, this investigation pertains to a complex financial crime. As such, information presented within this affidavit is approximate and based on the ongoing, evolving nature of the investigation. My understanding of the facts and circumstances presented within this affidavit may change over time, especially when considered in light of other evidence gathered during the investigation.

II. FACTS ESTABLISHING PROBABLE CAUSE

A. Summary of Investigation

9. Singh purports to be the head of two different corporations operating in California: Kryptoblocks Inc. ("Kryptoblocks") and Albot Technologies ("Albot"). In general summary, evidence obtained to date by the government indicates that Singh used his status as

Chief Executive Officer of Kryptoblocks to apply for and obtain from a federally insured financial institution called KeyPoint Credit Union (“KeyPoint”) more than \$3 million in subsequently forgiven loans that were earmarked for COVID-19 relief to small businesses meeting certain requirements.¹

10. In support of his applications, Singh submitted a range of apparently fraudulent documentation, including IRS forms that were never actually filed with that agency, payroll spreadsheets containing names and wages of employees who apparently resided outside the United States, and more. Some of Singh’s fraudulent loan applications indicated that the Subject Premises was the principal place of business for Kryptoblocks. Additionally, Singh submitted financial documentation in support of fraudulent loan applications that listed the Subject Premises as the address of Kryptoblocks. Other documentation uncovered by law enforcement personnel during this investigation indicates that Singh also claimed the Subject Premises as an address associated with Albot.

11. After Singh obtained millions of dollars in pandemic loans to Kryptoblocks from KeyPoint, he transferred much of the proceeds through personal bank accounts and corporate bank accounts linked to Kryptoblocks and Albot that he controlled. Singh spent a substantial portion of the loan proceeds he received on expenditures that were not authorized by the applicable loan program’s rules, such as personal expenses, residential mortgage payments, luxury goods, travel, and transfers to individuals located overseas.

B. Background on Paycheck Protection Program

12. At all relevant times, the United States Small Business Administration (the “SBA”) operated the Paycheck Protection Program (the “PPP”), a congressionally mandated program through which third-party lenders like KeyPoint funded forgivable loans to businesses in the United States affected by the COVID-19 pandemic. These loans were guaranteed by the United States Treasury and overseen by the SBA.

¹ I reviewed information maintained online by the National Credit Union Administration, which indicated that KeyPoint is federally insured by that entity.

13. PPP rules required prospective borrowers to certify, among other things:

- a) That an applicant business was in operation on February 15, 2020;
- b) That it employed workers for whom it paid salaries and payroll taxes or paid independent contractors as reported on IRS Form 1099-MISC;
- c) That the principal places of residence for employees of the applicant business were in the United States;
- d) The accuracy of the average monthly payroll expenses and number of employees of the applicant business; and
- e) The accuracy of information and documents submitted in support of the loan application.

14. PPP rules provided that loan proceeds could only be used for business payroll costs, business rent or mortgage costs, business utilities, or other business expenses.

15. In general, successful applicants for PPP loans received their loan proceeds directly from the financial institutions that processed their loan applications, and on terms that required the loans to be repaid over time at a low interest rate (around 1%). Loan recipients who demonstrated that they spent loan proceeds on allowable business expenses could seek to have their PPP loans entirely forgiven.

16. PPP rules required borrowers seeking forgiveness of their loans to certify, among other things:

- a) That PPP loan proceeds had been used to pay business costs eligible for forgiveness, such as payroll costs to retain employees, business utility payments, covered worker protection expenditures, and the like;
- b) That at least 60% of the amount for which the borrower sought forgiveness consisted of payroll costs;
- c) That the borrower verified the accuracy of the eligible payroll and nonpayroll costs for which forgiveness was sought; and

///

- d) The accuracy of information and documents submitted in support of the forgiveness application.

17. Applicants seeking PPP loans and their subsequent forgiveness generally submitted their applications directly to third-party financial institutions, such as KeyPoint, using the internet.

C. Singh successfully applied for a PPP loan of \$1.4 million.

18. In or around April 2020, KeyPoint received an application for a PPP loan to Kryptoblocks (the “First Draw” loan) that purported to be submitted over the internet by Singh. In support of this application, Singh represented the following, among other things:

- a) He was the Chief Executive Officer and sole owner of Kryptoblocks;
- b) The business phone number associated with the application was 650-391-8550 (the “8550 number”);²
- c) The taxpayer identification number associated with the application was Singh’s personal Social Security Number;
- d) The principal place of business for Kryptoblocks was the Subject Premises;
- e) Kryptoblocks employed eighty-four people, with an average monthly corporate payroll of over \$570,000;
- f) The United States was the principal place of residence for all employees used to calculate Kryptoblocks’s payroll; and
- g) Any loan proceeds would be used for Kryptoblocks’s payroll, rent or mortgage interest, or utilities.

19. In support of his application, Singh submitted what purported to be a true and accurate IRS Form W-3 showing that Kryptoblocks paid employee wages of more than \$9 million in 2019 and withheld more than \$1.3 million in federal income tax in 2019. However, ///

² According to records obtained by investigative personnel from Sprint, Singh was the owner of the 8550 number through at least April 2020.

according to records maintained by the IRS, Kryptoblocks did not report any income, payroll, or employees to the IRS between 2016 and 2024.

20. In or around May 2020, KeyPoint approved Singh's First Draw loan application and funded a loan of \$1,426,847.00 to Kryptoblocks. KeyPoint deposited the First Draw loan proceeds via interstate wire into a Kryptoblocks corporate bank account held at Bank of America, the account number for which ended in 8845 (the "8845 account").³ According to records provided by Bank of America, Singh opened the 8845 account in Sacramento in November 2019 and was the sole signatory on the account. At the time the First Draw loan proceeds were deposited into the 8845 account, the 8845 account had a balance of less than \$5,000.

21. Between May 2020 and August 2021, according to records provided to investigators for the 8845 account and for other financial accounts associated with Singh, Singh spent the majority of the First Draw loan proceeds on a variety of expenditures that were not authorized for PPP funds. These expenditures included regular payments on Singh's home mortgage; over \$1 million in direct transfers to individuals located in India; incidentals such as food, clothing, transportation, and luxury goods; and other personal expenses.

22. Based upon the foregoing, I submit that probable cause exists to believe that Singh violated 18 U.S.C. §§ 1343 and 1344 by using the internet to submit a PPP loan application to a federally insured credit union that contained material misrepresentations, and that involved an interstate wire transmission.

1. Forgiveness of First Draw Loan

23. In or around October 2021, KeyPoint received an application for forgiveness of the First Draw loan issued to Kryptoblocks, which again purported to be submitted by Singh. In support of his forgiveness application, Singh represented the following, among other things:

³ The investigation indicates this wire was made using Fedwire, a system operated by the Federal Reserve. I am aware, based upon my training, experience, and consultation with others, that Fedwire transactions since 2015 involve two separate computer servers, one in Texas, and the other in New Jersey.

- a) The 8550 number was the business phone number associated with Kryptoblocks's application;
- b) The taxpayer identification number associated with the application was Kryptoblocks's federal Employer Identification Number;
- c) The Subject Premises was the business address for Kryptoblocks;
- d) At the time of its application for forgiveness of the First Draw loan, Kryptoblocks employed ninety people; and
- e) Between May and October 2020, Kryptoblocks paid \$1,426,847.00 in payroll to employees whose principal places of residence were in the United States.

24. To substantiate the certifications made on the application for forgiveness of the First Draw loan, Singh sent KeyPoint personnel what purported to be true and accurate documents, including the following:

- a) An IRS Form 940 for 2020 bearing Singh's name and the 8550 number and purporting to show that Kryptoblocks paid \$9.2 million in wages, requiring it to remit \$3,738 to the IRS in federal unemployment tax that year;
- b) An IRS Form 941 for the second quarter of 2020, bearing Singh's name and the 8550 number and purporting to show that Kryptoblocks paid more than \$2 million in employee wages that quarter and withheld more than \$650,000 in federal income tax that same quarter;
- c) An IRS Form 941 for the third quarter of 2020, bearing Singh's name and the 8550 number and purporting to show that Kryptoblocks paid more than \$2 million in employee wages that quarter and withheld more than \$650,000 in federal income tax that same quarter; and
- d) A spreadsheet purporting to show that Kryptoblocks employed eighty-eight people to whom it paid more than \$9 million in wages (along with associated federal and California taxes) in 2019 and \$3 million in wages (along with associated federal and California taxes) in 2020, including approximately

\$110,000 paid to Singh himself, \$106,000 paid to Singh's wife Neelam Singh, and \$95,000 paid to Singh's brother Neeraj Masih.⁴

25. However, according to records maintained by the IRS, Kryptoblocks did not report any income, payroll, or employees to the IRS between 2016 and 2024. Additionally, according to records obtained by investigators from the California Employment Development Department (the "EDD"), Kryptoblocks did not report any wages paid to employees in California in 2020. And according to information provided to investigators by the California Franchise Tax Board (the "FTB"), Kryptoblocks did not file a California corporate tax return for 2019 or 2020.

26. Furthermore, according to bank records for the 8845 account, Singh did not make any payments to tax authorities from this account in 2019 or 2020.

27. In or around October 2021 and based on Singh's representations in support of his First Draw loan forgiveness application, KeyPoint requested that the SBA forgive the First Draw loan previously extended to Kryptoblocks. That same month, the SBA forgave the First Draw loan in full.

28. Based upon the foregoing, I submit that probable cause exists to believe that Singh violated 18 U.S.C. § 1344 by submitting a false First Draw loan forgiveness application to KeyPoint.

D. Singh successfully applied for a second PPP loan of \$1.9 million.

29. In or around January 2021, Singh used the internet to submit an application to KeyPoint for a subsequent PPP loan to Kryptoblocks (the "Second Draw" loan). In support of his application, Singh represented the following, among other things:

- a) He was the Chief Executive Officer and sole owner of Kryptoblocks;
- b) The business phone number associated with the application was the 8550 number;
- c) The taxpayer identification number associated with the application was Kryptoblocks's federal Employer Identification Number;

⁴ Singh reported that Neelam Singh was his spouse and that Neeraj Masih was his brother on tax returns filed with the IRS that were reviewed as part of this investigation.

- d) The principal place of business for Kryptoblocks was an address in an office building on Promenade Circle in Sacramento, which is located less than two miles from the Subject Premises and which currently houses a lending company doing business as Regional Finance;
- e) Kryptoblocks maintained an average monthly payroll of approximately \$838,911.00;
- f) Kryptoblocks employed eighty-nine people;
- g) Kryptoblocks sought a Second Draw loan to pay for eligible payroll costs, rent/mortgage interest, utilities, and covered operations expenditures;
- h) The United States was the principal place of residence for all employees included in Kryptoblocks's payroll calculation; and
- i) Kryptoblocks used its First Draw loan proceeds only on eligible expenses.

30. In support of the Second Draw loan application, Singh submitted a bank statement for the 8845 account displaying the Subject Premises as the contact address for Kryptoblocks and demonstrating the withdrawal of approximately \$86,000 from that account in January 2021.

31. KeyPoint's loan file for the Second Draw loan also includes the following documents:

- a) An IRS Form 940 for 2019 displaying the Subject Premises and the 8550 number, and purporting to show that Kryptoblocks paid \$9.2 million in wages;
- b) An IRS Form W-3 for 2019 displaying the 8550 number, and purporting to show that Kryptoblocks paid more than \$9 million in wages and withheld more than \$1.3 million in federal income tax that year;
- c) A purportedly true and accurate profit-and-loss statement showing that Kryptoblocks generated more than \$17 million in net revenue in 2019 and more than \$12 million in net revenue in 2020; and
- d) A purportedly true and accurate spreadsheet showing that Kryptoblocks employed eighty-eight people to whom it paid more than \$9 million in wages (along with

associated federal and California taxes) in 2020, including to Singh himself, Singh's wife, and Singh's brother.

32. However, according to records maintained by the IRS, Kryptoblocks did not report any income, payroll, or employees to the IRS between 2016 and 2024. Additionally, according to records obtained by investigators from the EDD, Kryptoblocks did not report making any wage payments to California employees in 2020. And according to records obtained by investigators from the FTB, Kryptoblocks did not file a California corporate tax return for 2019 or 2020.

33. In or around March 2021, KeyPoint approved Singh's Second Draw loan application and funded a loan of \$1,990,152.00 to Kryptoblocks. KeyPoint deposited these Second Draw loan proceeds via interstate wire transfer into a Kryptoblocks corporate bank account held at Bank of America, the account number for which ended in 5717 (the "5717 account").⁵ According to records received from Bank of America, Singh opened the 5717 account in Sacramento in May 2020 and was the sole signatory on the account. At the time the Second Draw loan proceeds were deposited into the 5717 account, that account had a balance of less than \$2,500.

34. Based upon the foregoing, I submit that probable cause exists to believe that Singh violated 18 U.S.C. §§ 1343 and 1344 by using the internet to submit a Second Draw loan application to a federally insured credit union that contained material misrepresentations, and that involved an interstate wire transmission.

1. Expenditures of Second Draw Loan Proceeds

35. Between March 2021 and February 2022, nearly all of the proceeds Kryptoblocks received from the Second Draw loan were spent from the 5717 account. According to records provided to investigators for the 5717 account, Singh spent some of the Second Draw loan
///

⁵ This transaction was made using Fedwire and therefore involved an interstate wire transmission.

proceeds on expenditures that could qualify as legitimate uses of PPP funds, such as payments to business solutions providers like Amazon Web Services, Apple, Google, Atlassian, and the like.

36. However, according to records provided to investigators for the 5717 account and for other financial accounts associated with Singh, Singh spent much of the Second Draw loan proceeds on a variety of expenditures that do not appear to have been authorized for PPP funds. These expenditures included:

- a) Hundreds of thousands of dollars in transfers to an Albot corporate bank account for which Singh was the sole signatory;
- b) Transfers to other companies such as engineering and biosciences firms, one of which issued a press release in or around June 2021 touting its partnership with Albot to distribute COVID-19 diagnostic testing kits;
- c) Tens of thousands of dollars of transfers to a personal banking account held at Bank of America on which Singh and his wife were the sole signatories;
- d) Incidentals such as food, clothing, and luxury goods; and
- e) An approximately \$500,000 payment to Singh's home mortgage lender made in mid-August of 2021.

37. I conducted a tracing of the proceeds of Kryptoblocks' Second Draw loan using an accounting method approved by the Money Laundering and Asset Recovery Section of the United States Department of Justice. This tracing analysis revealed that the approximately \$500,000 payment to Singh's mortgage lender necessarily contained greater than \$10,000 of the proceeds of Singh's fraudulent conduct in obtaining the Second Draw loan. Thus, I submit that probable cause exists to believe that Singh violated 18 U.S.C. § 1957 by conducting this financial transaction using more than \$10,000 of funds derived from his fraudulent scheme.

2. Forgiveness of Second Draw Loan

38. In or around February 2022, Singh used the internet to submit an application to KeyPoint for forgiveness of the Second Draw loan issued to Kryptoblocks. In support of his forgiveness application, Singh certified the following, among other things:

- a) The business phone number associated with the application was the 8550 number;
- b) The taxpayer identification number associated with the application was Kryptoblocks's federal Employer Identification Number;
- c) The principal place of business for Kryptoblocks was the Subject Premises;
- d) At the times of its application for the Second Draw loan and for its subsequent forgiveness, Kryptoblocks employed 101 people;
- e) Between March and September 2021, Kryptoblocks paid its employees over \$5 million in wages; and
- f) Kryptoblocks used its Second Draw loan for payroll costs paid to employees.

39. To substantiate the certifications he made on his application for forgiveness of the Second Draw loan, Singh submitted various documents to KeyPoint that he purported to be true, including the following:

- a) An IRS Form 941 for the first quarter of 2021, displaying the Subject Premises and the 8550 number and purporting to show that Kryptoblocks paid more than \$2.6 million in employee wages that quarter and withheld more than \$744,000 in federal payroll taxes that same quarter;
- b) An IRS Form 941 for the second quarter of 2021, displaying the Subject Premises and the 8550 number and again purporting to show that Kryptoblocks paid more than \$2.6 million in employee wages that quarter and withheld more than \$744,000 in federal payroll taxes that same quarter;
- c) An IRS Form 941 for the third quarter of 2021, displaying the Subject Premises and the 8550 number and again purporting to show that Kryptoblocks paid more than \$2.6 million in employee wages that quarter and withheld more than \$744,000 in federal payroll taxes that same quarter; and
- d) A spreadsheet purporting to show that Kryptoblocks employed ninety-nine people to whom it paid more than \$10 million in wages (along with associated federal and California taxes) in 2021, including more than \$110,000 paid to Singh

himself, more than \$106,000 paid to Singh's wife, and more than \$95,000 paid to Singh's brother.

40. However, according to records maintained by the IRS, Kryptoblocks did not report any income, payroll, or employees to the IRS between 2016 and 2024. And according to records obtained by investigators from the EDD, Kryptoblocks did not report making any wage payments to employees in 2021. Additionally, according to information provided to investigators by the FTB in 2022, Kryptoblocks did not file a corporate tax return with the State of California for 2021. Furthermore, according to bank records for the 8845 account and the 5717 account, Singh did not make any payments to tax authorities from these accounts in 2020 or 2021.

41. In or around March 2022 and based on Singh's representations in support of his Second Draw loan forgiveness application, KeyPoint requested that the SBA forgive the Second Draw loan previously extended to Kryptoblocks. In April 2022, the SBA forgave the Second Draw loan in full.

42. Based upon the foregoing, I submit that probable cause exists to believe that Singh violated 18 U.S.C. § 1344 by submitting a false Second Draw loan forgiveness application to KeyPoint.

E. Additional Facts Regarding Singh and the Subject Premises

43. I reviewed records obtained during the investigation from various financial institutions, government agencies, and other reliable sources. These records revealed the following facts tying Singh to the Subject Premises.

1. Economic Injury Disaster Loan Applications

44. Between March 2020 and October 2021, the SBA received three Economic Injury Disaster Loan ("EIDL") applications for Kryptoblocks. Each of these applications listed Singh as the owner of Kryptoblocks and represented that the business employed between twenty and 120 employees. Each of these applications also provided the 8550 number as the business phone number and claimed that the primary business address was the Subject Premises.

///

45. In or around April 2020, Singh submitted a PPP loan application from Kryptoblocks to a financial institution doing business as Ready Capital. This application displayed Singh's name, the Subject Premises, and the 8550 number.

46. In or around December 2021, the SBA received three EIDL applications for Albot. Each of these applications listed Singh as the business owner of Albot and represented that the business employed between ten and 132 employees. Each of these applications also provided the 8550 number as the business phone number and claimed that the primary business address was the Subject Premises.

2. Financial and Public Records

47. Records provided by Bank of America revealed the following:

- a) The Subject Premises was listed as the physical address connected to the 8845 account between May 2020 and the account's closure in approximately August 2022;
- b) The Subject Premises was listed as the physical address connected to the 5717 account between May 2020 and the account's closure in August 2022;
- c) The Subject Premises was listed as the physical address connected to an account in the name of Singh and his wife Neelam Singh between February 2020 and approximately May 2024;
- d) The Subject Premises was listed as the physical address connected to an Albot corporate bank account between April 2021 and the account's closure in approximately July 2022.

48. California Department of Motor Vehicles records indicate that Singh's most recent residence is the Subject Premises.

49. Records obtained from Bank of America indicate that Singh frequently uses online banking features to conduct monetary transactions, such as personal and external account transfers. Other records from Bank of America indicate that financial accounts belonging to Kryptoblocks and Albot were frequently accessed via a mobile electronic device such as a

smartphone. Hence, I believe that Singh uses an electronic device, most likely a smartphone, with the Bank of America application installed on it to access accounts relevant to this investigation.

3. Surveillance

50. On or about December 31, 2024, law enforcement agents conducted observation of the Subject Premises and saw a champagne white Honda CRV bearing California license plate 5XHB385 parked in front of the Subject Premises. A license plate check on the white Honda's motor vehicle record revealed that the vehicle is registered to Singh or his wife Neelam Singh at the Subject Premises.

51. On or about February 3, 2025, law enforcement agents conducted further observation of the Subject Premises and observed Singh depart the Subject Premises at approximately 9:56 a.m. in a black Acura RDX registered in Singh's name.

III. COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

52. As described above and in Attachment B, this application seeks permission to search for records that might be found on Singh's person or on the Subject Premises (including on relevant digital devices found inside), in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrants for which I am applying would authorize the seizure and subsequent search of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure.

1. Probable Cause

53. I submit that if a computer or storage medium is found on the Subject Premises or on Singh's person, there is probable cause to believe relevant records will be stored on that computer or storage medium, for at least the following reasons.

54. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the internet. Electronic files downloaded to a

storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

55. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

56. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

57. Similarly, files that have been viewed via the internet are sometimes automatically downloaded into a temporary internet directory or “cache.”

58. Based on actual inspection of other evidence related to this investigation (including electronically stored and transmitted spreadsheets, financial records, tax documents, and other business-related documents), I am aware that computer equipment was used to generate, store, and print documents used in Singh’s fraud and money laundering scheme under investigation. Hence, I submit that there is probable cause to believe that there is a computer system currently located on the Subject Premises.

2. Forensic Evidence

59. As further described in Attachment B, this application seeks permission to locate not only computer files and information that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how

computers were used, the purpose of their use, who used them, and when. I submit that there is probable cause to believe that this forensic electronic evidence will be on any storage medium in the Subject Premises for the following reasons.

60. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

61. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the government to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (such as registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner.

62. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log computer user account session times and durations,

computer activity associated with user accounts, electronic storage media that connected with the computer, and the Internet Protocol (“IP”) addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation.

63. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (such as a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user.

64. Last, information stored within a computer may provide relevant insight into the computer user’s state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner’s motive and intent to commit a crime (such as internet searches indicating criminal planning), or consciousness of guilt (such as running a “wiping” program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

65. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

66. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and

passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrants for which I am applying.

67. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

68. Based on my training and experience, I know that when an individual uses a computer to submit fraudulent documentation in furtherance of a financial fraud scheme, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of internet discussions about the crime; and other records that indicate the nature of the offense.

3. Necessity of Seizing or Copying Entire Computers or Storage Media

69. In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following facts.

70. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrants call for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrants can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

71. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Subject Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

72. Records sought under these warrants could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools. Based on the foregoing, and consistent with Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, the warrants I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrants, and would authorize a later review of the media or information consistent with the warrants. The latter review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

73. Because it appears likely that Singh's wife (and possibly his brother) share the Subject Premises as a residence with Singh himself, it is possible that the Subject Premises will contain storage media that are predominantly used, and perhaps owned, by persons who are not

suspected of a crime. Based on my training and experience, I know that digital devices can be located in any area of a shared residence and that digital devices can be shared by cohabitants. I am not aware of any areas of the Subject Premises to which Singh lacks access or in which it would be impossible for him to store evidence. The warrants for which I am applying would authorize the seizure of such devices that are reasonably believed to belong to Singh or to have been used in the offenses under investigation. If a forensic review determines that there is no evidence of the suspected crimes on a computer or storage media, reasonable efforts will be made to return the items to their owners.

74. Based on what I know of them from this investigation, Kryptoblocks and Albot could conduct legitimate business in addition to being tools of Singh's fraud. The seizure of computers used to conduct business by Kryptoblocks or Albot may limit those companies' abilities to conduct legitimate business. As with any search warrant, I expect that these warrants will be executed reasonably. Reasonable execution will likely involve conducting an investigation on the scene of what computers, or storage media, must be seized or copied, and what computers or storage media need not be seized or copied. Where appropriate, officers will copy data, rather than physically seize computers, to reduce the extent of disruption. If employees of Kryptoblocks or Albot so request, executing agents will, to the extent practicable, attempt to provide employees with copies of data that may be necessary or important to the continuing function of those companies' legitimate business. If, after inspecting the computers, it is determined that some or all of this equipment is no longer necessary to retrieve and preserve the evidence, the government will return it.

IV. CONCLUSION AND REQUEST FOR SEALING

75. I respectfully request that search warrants be issued authorizing a search of Singh and the Subject Premises, as further described within Attachments A-1 and A-2, and the seizure of the items set forth in Attachment B.

76. I further request that the Court order that all papers in support of this application, including the affidavit and search warrants, be sealed. These documents discuss an ongoing

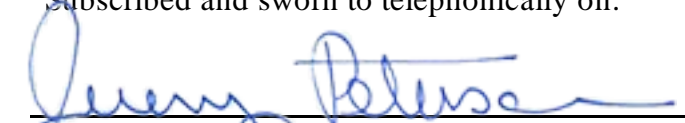
criminal investigation that is neither public nor known to Singh. Accordingly, I submit that there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Respectfully submitted,

/s/ Marshall Miller

Marshall Miller
Special Agent
Internal Revenue Service-Criminal Investigation

Subscribed and sworn to telephonically on: February 18, 2025


THE HONORABLE JEREMY D. PETERSON
United States Magistrate Judge

/s/ Sam Stefanki

Approved as to form by AUSA SAM STEFANKI

ATTACHMENT A-1

Person to Be Searched



The person to be searched is Akash Kumar Singh, born February 11, 1977, a citizen of India and legal permanent resident of the United States.

Akash Kumar Singh is identified in California Department of Motor Vehicles records as standing five feet, eight inches tall, weighing 165 pounds, with brown hair and brown eyes. The image of Singh depicted above is a true and accurate representation of the image of Singh on file with the California Department of Motor Vehicles and was taken on or about March 9, 2021.

ATTACHMENT A-2

Property to Be Searched



The property to be searched is the single-family residence located at 2484 Amelia Earhart Avenue, Sacramento, California 95834 (the “Subject Premises”).

The Subject Premises is a multi-story home located in a suburban neighborhood in the Natomas area of Sacramento. The home is situated west of Samuelson Way and east of John W Young Street. Open-source information and information associated with the Subject Premises indicates the Subject Premises is approximately 2,486 square feet with four bedrooms and four bathrooms. The property to be searched includes the entire residence as well as the grounds surrounding the home, including any outbuildings, garages, or sheds, as well as any motor vehicles, boats, trailers, or off-road vehicles provided that they are parked on the property itself.

The photograph above was taken from a public roadway by a special agent of the Internal Revenue Service-Criminal Investigation in December 2024.

ATTACHMENT B

Items to Be Seized

1. All records relating to violations of 18 U.S.C. §§ 1343, 1344, and/or 1957, those violations involving Paycheck Protection Program loans and/or Economic Injury Disaster Loans applied for by, or paid to, Akash Kumar Singh, Kryptoblocks, or Albot (the “Subject Businesses”) and occurring from January 1, 2020, to the date of this search warrant, including:

- a) Recordings relating to financial loan application forms;
- b) Records relating to IRS forms (including IRS Forms 940, 941, 1120, 1120-S, 1065, W-2, W-3, and the like);
- c) Correspondence with banks and government agencies regarding those loans, as well as records revealing where proceeds of those loans were spent or transferred;
- d) Records relating to Akash Kumar Singh and the Subject Businesses’ sources of income and/or employment, federal and state tax returns, and related federal and state tax records;
- e) Records relating to employees, purported employees, or independent contractors of the Subject Businesses, or of other business concerns associated with Akash Kumar Singh, including employee payroll records, employee rosters, wage/hour tracking sheets, payroll tax returns, tax withholding records, IRS Forms W-2 or 1099, pay checks, or earnings/leave statements;
- f) Records relating to bank or financial transactions, including any bank records pertaining to Akash Singh and the Subject Businesses such as statements, correspondence, deposit slips, check registers, cancelled checks, withdrawals, ATM receipts, ATM/credit cards, prepaid debit cards, certificates of deposit, cashed check receipts, receipts for purchases made with debit and/or credit cards, wire transfer receipts, cashier’s checks, cashier’s check receipts, United States Treasury checks, debit and credit memos, safe deposit and/or storage locker keys, safes, or other bank records;
- g) Records relating to any of the following for Akash Kumar Singh, Neelam Singh, or Neeraj Masih: personal credit card statements, credit card payments, loan applications, loan and debt agreements, loan payments, lines of credit, and records relating to payment of debt;
- h) Records relating to financial bookkeeping or accounting by Akash Singh or the Subject Businesses, including income statements, balance sheets, general ledgers, general journals, gross receipts records, income records, cash receipts records, cash receipts schedules, records of payments or deposits, disbursement records and/or journals, loan receivable and loan payable ledgers, and any business documents required by state or federal law to be filed or maintained by a business;

- i) Records relating to any accounts created with the United States Small Business Administration or any financial services company, bank, or other government agency involved in COVID-19 relief;
 - j) Business cards, flyers, promotional materials, or other documents describing the condition, mission, clients, or employees of Akash Singh or the Subject Businesses;
 - k) Records relating to or showing the disposition of any monetary or financial transaction involving COVID-19 relief funds, grants, loans, or other proceeds conducted by Akash Singh or an employee or agent of the Subject Businesses; and
 - l) Records relating to purchase or sale of personal items, vehicles, luxury items (such as jewelry, watches, electronics, and handbags), residences, or other items potentially purchased with fraud proceeds, including purchase agreements, installment agreements, layaway paperwork, invoices, or receipts.
2. Records relating to the destruction, deletion, removal, or concealment of other records.
3. Records relating to accessing electronic devices or cryptocurrency, such as passwords, password files, test keys, encryption codes, or other access keys.
4. Articles of personal property tending to establish the identity of the person or persons in control of the Subject Premises, including:
- a) Identity documents;
 - b) Passports;
 - c) Legal resident cards;
 - d) Visas;
 - e) Driver licenses;
 - f) Rent or mortgage receipts;
 - g) Loan documents;
 - h) Lease agreements;
 - i) Utility bills or receipts;
 - j) Addressed envelopes;
 - k) Internet service bills or communications from internet service providers; and

- l) Telephone or cellular phone bills.

5. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, “computer”):

- a) Evidence of who used, owned, or controlled the computer at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
- b) Evidence of software that would allow others to control the computer, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c) Evidence of the lack of such malicious software;
- d) Evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- e) Evidence of the attachment to the computer of other storage devices or similar containers for electronic evidence;
- f) Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the computer;
- g) Evidence of the times the computer was used;
- h) Passwords, encryption keys, and other access devices that may be necessary to access the computer;
- i) Documentation and manuals that may be necessary to access the computer or to conduct a forensic examination of the computer;
- j) Records of or information about Internet Protocol addresses used by the computer;
- k) Records of or information about the computer’s internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any internet search engine, and records of user-typed web addresses; and
- l) Routers, modems, and network equipment used to connect computers to the internet.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the executing agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

UNITED STATES DISTRICT COURT

for the
Eastern District of California

In the Matter of the Search of

2484 AMELIA EARHART AVENUE,
SACRAMENTO, CALIFORNIA 95834

Case No. 2:25-sw-0135 JDP

SEALED

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the _____ Eastern _____ District of _____ California
(identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A-2, attached hereto and incorporated by reference.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (*identify the person or describe the property to be seized*):

SEE ATTACHMENT B, attached hereto and incorporated by reference.

YOU ARE COMMANDED to execute this warrant on or before March 4, 2025, *(not to exceed 14 days)*

☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to: any authorized U.S. Magistrate Judge in the Eastern District of California.

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (*check the appropriate box*)

☐ for _____ days (*not to exceed 30*) ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: February 18, 2025 at 4:46 p.m.

City and state: Sacramento, California

_____, the later specific date of _____.



Judge's signature

Jeremy D. Peterson, U.S. Magistrate Judge

Printed name and title

Return

Case No.:

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I swear that this inventory is a true and detailed account of the person or property taken by me on the warrant.

Subscribed, sworn to, and returned before me this date.

Signature of Judge

Date

ATTACHMENT A-2

Property to Be Searched



The property to be searched is the single-family residence located at 2484 Amelia Earhart Avenue, Sacramento, California 95834 (the “Subject Premises”).

The Subject Premises is a multi-story home located in a suburban neighborhood in the Natomas area of Sacramento. The home is situated west of Samuelson Way and east of John W Young Street. Open-source information and information associated with the Subject Premises indicates the Subject Premises is approximately 2,486 square feet with four bedrooms and four bathrooms. The property to be searched includes the entire residence as well as the grounds surrounding the home, including any outbuildings, garages, or sheds, as well as any motor vehicles, boats, trailers, or off-road vehicles provided that they are parked on the property itself.

The photograph above was taken from a public roadway by a special agent of the Internal Revenue Service-Criminal Investigation in December 2024.

ATTACHMENT B

Items to Be Seized

1. All records relating to violations of 18 U.S.C. §§ 1343, 1344, and/or 1957, those violations involving Paycheck Protection Program loans and/or Economic Injury Disaster Loans applied for by, or paid to, Akash Kumar Singh, Kryptoblocks, or Albot (the “Subject Businesses”) and occurring from January 1, 2020, to the date of this search warrant, including:

- a) Recordings relating to financial loan application forms;
- b) Records relating to IRS forms (including IRS Forms 940, 941, 1120, 1120-S, 1065, W-2, W-3, and the like);
- c) Correspondence with banks and government agencies regarding those loans, as well as records revealing where proceeds of those loans were spent or transferred;
- d) Records relating to Akash Kumar Singh and the Subject Businesses’ sources of income and/or employment, federal and state tax returns, and related federal and state tax records;
- e) Records relating to employees, purported employees, or independent contractors of the Subject Businesses, or of other business concerns associated with Akash Kumar Singh, including employee payroll records, employee rosters, wage/hour tracking sheets, payroll tax returns, tax withholding records, IRS Forms W-2 or 1099, pay checks, or earnings/leave statements;
- f) Records relating to bank or financial transactions, including any bank records pertaining to Akash Singh and the Subject Businesses such as statements, correspondence, deposit slips, check registers, cancelled checks, withdrawals, ATM receipts, ATM/credit cards, prepaid debit cards, certificates of deposit, cashed check receipts, receipts for purchases made with debit and/or credit cards, wire transfer receipts, cashier’s checks, cashier’s check receipts, United States Treasury checks, debit and credit memos, safe deposit and/or storage locker keys, safes, or other bank records;
- g) Records relating to any of the following for Akash Kumar Singh, Neelam Singh, or Neeraj Masih: personal credit card statements, credit card payments, loan applications, loan and debt agreements, loan payments, lines of credit, and records relating to payment of debt;
- h) Records relating to financial bookkeeping or accounting by Akash Singh or the Subject Businesses, including income statements, balance sheets, general ledgers, general journals, gross receipts records, income records, cash receipts records, cash receipts schedules, records of payments or deposits, disbursement records and/or journals, loan receivable and loan payable ledgers, and any business documents required by state or federal law to be filed or maintained by a business;

- i) Records relating to any accounts created with the United States Small Business Administration or any financial services company, bank, or other government agency involved in COVID-19 relief;
 - j) Business cards, flyers, promotional materials, or other documents describing the condition, mission, clients, or employees of Akash Singh or the Subject Businesses;
 - k) Records relating to or showing the disposition of any monetary or financial transaction involving COVID-19 relief funds, grants, loans, or other proceeds conducted by Akash Singh or an employee or agent of the Subject Businesses; and
 - l) Records relating to purchase or sale of personal items, vehicles, luxury items (such as jewelry, watches, electronics, and handbags), residences, or other items potentially purchased with fraud proceeds, including purchase agreements, installment agreements, layaway paperwork, invoices, or receipts.
2. Records relating to the destruction, deletion, removal, or concealment of other records.
3. Records relating to accessing electronic devices or cryptocurrency, such as passwords, password files, test keys, encryption codes, or other access keys.
4. Articles of personal property tending to establish the identity of the person or persons in control of the Subject Premises, including:
- a) Identity documents;
 - b) Passports;
 - c) Legal resident cards;
 - d) Visas;
 - e) Driver licenses;
 - f) Rent or mortgage receipts;
 - g) Loan documents;
 - h) Lease agreements;
 - i) Utility bills or receipts;
 - j) Addressed envelopes;
 - k) Internet service bills or communications from internet service providers; and

- l) Telephone or cellular phone bills.

5. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, “computer”):

- a) Evidence of who used, owned, or controlled the computer at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
- b) Evidence of software that would allow others to control the computer, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c) Evidence of the lack of such malicious software;
- d) Evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- e) Evidence of the attachment to the computer of other storage devices or similar containers for electronic evidence;
- f) Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the computer;
- g) Evidence of the times the computer was used;
- h) Passwords, encryption keys, and other access devices that may be necessary to access the computer;
- i) Documentation and manuals that may be necessary to access the computer or to conduct a forensic examination of the computer;
- j) Records of or information about Internet Protocol addresses used by the computer;
- k) Records of or information about the computer’s internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any internet search engine, and records of user-typed web addresses; and
- l) Routers, modems, and network equipment used to connect computers to the internet.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the executing agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.